## REMARKS

The final Office Action, mailed July 21, 2006, considered and rejected claims 1-25. Claims 1-6, 8-13, 15-23 and 25 were rejected under 35 U.S.C. 103(a) as being unpatentable over CERT CC, "Cert Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests" (CERT I) in view of CERT CC, "Understanding Malicious Content Mitigation for Web Developer" (CERT II), and further in view of Hidalgo (U.S. Publ. No. 2002/0051142) and "Hypertext Transfer Protocol – HTTP/1.1", RFC 2616 by Fielding et al. (Fielding). Claims 7, 14 and 24 were rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of CERT I, CERT II, Hidalgo and Fielding in view of Fischman et al. (U.S. Publ. No. 2003/0097588).[1]

The Office Action further rejected claims 1-25 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement, and objected to the specification for the claims not providing antecedent basis for the claim terminology, under M.P.E.P. § 608.01(o). Applicants respectfully submit that in light of the claim amendments reflected above, the rejections are now moot.[2]

The Office Action also objected to Figure 1 of the present application, and requested corrected drawings designating the figure as "Prior Art." Applicants note that amended drawings are being submitted herewith to denote Figure 1 as "Prior Art" and, accordingly, respectfully submit that this objection is now moot.

By this paper, claims 1, 8 and 18 have been amended, claims 26-29 added, and claims 13

---

[1] Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] Applicants do not, however, acquiesce to the assertions made in the Office Action with regard to the objection to the specification. In particular, Applicants note that the objection made in the Office Action in accordance with M.P.E.P. § 608.01(o) and 37 C.F.R. § 1.75(d)(1) is appropriate only where "new terms are introduced" and the "nomenclature [of the application as filed] is departed from by amendment of the claims". M.P.E.P. § 608.01(o). Applicants have reviewed the claims as previously presented, and as amended, and respectfully submit that the nomenclature is entirely consistent with the nomenclature of the application as originally filed. If the Office believes a particular term is not used within the original application, a recitation of the particular term is requested, rather than a recitation of the entire claim limitation, so as to give Applicants a chance to meaningfully respond. If a new matter rejection is intended, Applicants submit that a rejection in accordance with M.P.E.P. § 706.03(o) is more appropriate so as to advise Applicants of the actual basis of the rejection.

and 23 have been cancelled.[3]  Accordingly, following this paper, claims 1-12, 14-22 and 24-29 remain pending, of which claims 1, 8 and 18 are the only independent claims at issue.

Applicants' invention is directed to methods and computer program products for enabling a server to mitigate cross-scripting attacks.  As recited in claim 1, for example, a request is received from a user computer that includes data derived from an outside source.  Thereafter, a determination is made as to whether the request from the user computer includes a marker of active content.  If a marker of active content is included, the method includes refraining from serving a response to the request, and instead informing the user computer that a marker of active content has been discovered in the request.  Further, a request can be made for the user computer to resubmit the request so as to subsequently serve a response to a request resubmitted by the user computer.

Claims 8 and 18 are directed to a method and computer program product, respectively, and generally correspond to the method of claim 1, in a particular instance in which the request is an.HTTP request received by a server computer, and wherein serving the response to the request includes dynamically rendering a response to the HTTP request.

While the cited CERT I, CERT II and Hidalgo references generally relate to cross-site scripting, Applicants respectfully submit that, whether alone or in combination with the Fielding reference (which does not relate to cross-site scripting, but only to user errors), they fail to disclose or suggest the present invention.  For example, among other things, CERT I, CERT II and Hidalgo fail to disclose or suggest refraining from serving a response to the request if the request includes the marker of active content, and instead serving a response only to a request resubmitted by the user computer, as recited in combination with the other claim elements.

In fact, and in direct contrast to the above claims, CERT I and CERT II specifically teach that rather than aborting the request so as to refrain from serving a response, the request is processed and a response is in fact returned.  For example, CERT I generally discusses the problem associated with malicious code from cross-site scripting attacks (p. 1-2), and notes that web site developers can prevent such attacks by allowing only a limited character set or by filtering data *during generation of the output page.*  (p. 5, ¶ 3-6).  Thus, CERT I teaches that

---

[3] Support for the claim amendments can be found throughout the specification, including, but not limited to, the disclosure found in originally filed paragraphs [0006], [0007] and [0024]-[0031].

while filtering for script characters is performed, an output page is generated. For additional details on encoding and filtering, however, CERT I refers to the CERT II document.

CERT II further expounds on a manner in which cross-site scripting attacks can be minimized by filtering specific characters out of web pages that contain both text and HTML markup. (p. 1, ¶¶ 1-2, Problem Summary; p. 4, ¶¶ 3-4). For example, a web page request may be filtered either during the data input or the data output process to ensure that all dynamic content is filtered. (p. 4, ¶ 4). CERT II further provides three examples of code to perform the requested filtering. As clearly shown in the JavaScript example on p. 5, a string of characters (InStr) in a request is examined for particular characters (e.g. < > " ' % ; ( ) & +). When any such character is encountered, it is replaced by a null value by the "InStr.replace" function. The string of characters is then returned by the "return InStr" function, which results in the "bad" characters being removed, but which still includes any character which is not defined as a "bad" character. Similar examples are disclosed in C++ and PERL examples, in which bad characters are defined and filtered out, but in which a return of "good" characters is still made.

Thus, the CERT I and CERT II references disclose that characters within a request are filtered and replaced, and further expressly teaches that even in the presence of such characters, the request is still processed, and a filtered result is rendered and presented. In other words, when a request is received, CERT I and CERT II teach that all the "bad" characters in the request are removed, but that all of the "good" characters of the request are still processed and served to the user in a response. This is in fundamental contrast to Applicants claimed invention in which, rather than presenting a response with neutralized script characters, as described in CERT I and CERT II, a server of the present invention refrains from serving any response when a script construct or marker of active content is identified. Further, inasmuch as the teachings of CERT I and CERT II are in direct contrast to the teachings of the present invention, Applicants respectfully submit that there is no motivation to combine such references with another reference purportedly teaching aborting or otherwise refraining from executing a script when encountered, as recited in combination with the other claim elements.

In view of the foregoing, Applicants respectfully submit that the remaining rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. Nevertheless, Applicants further respectfully submit that the various new claims are also distinguishable over the art of record. For example, Applicants submit that the cited references fail
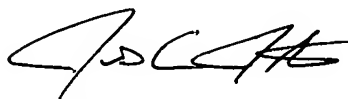
to teach wherein determining if a request from the user computer includes a marker of active content includes: evaluating only user input fields of the request (claim 26), or maintaining a list of markers of active content and inactivating markers in the list (claim 27). Moreover, while the CERT references identify various characters which can be filtered, they fail to disclose that an HTTP request is evaluated for a script construct comprising an onclick event (claim 28) or an element size expression (claim 29).

Although only the independent claims and the various new claims have been specifically addressed, it will be appreciated that this should not be construed as Applicants acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any Official Notice. Instead, Applicants reserve the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicants specifically request that the Examiner provide references supporting the teachings officially noticed, as well as provide the required motivation or suggestion to combine the relied upon notice with the other art of record.

For at least the foregoing reasons, Applicants respectfully submit that the pending claims are neither anticipated by nor made obvious by the art of record. In the event that the Examiner finds and remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 21<sup>st</sup> day of September, 2006.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
COLBY C. NUTTALL
Registration No. 58,146
Attorneys for Applicant
Customer No. 047973

RDN:JCJ:CCN

## AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Figure 1. This sheet, which includes

Figures 1 and 2, replaces the original sheet including Figures 1 and 2.


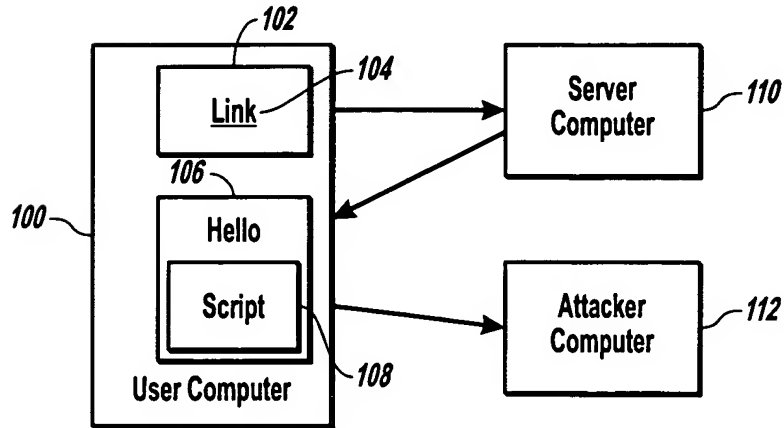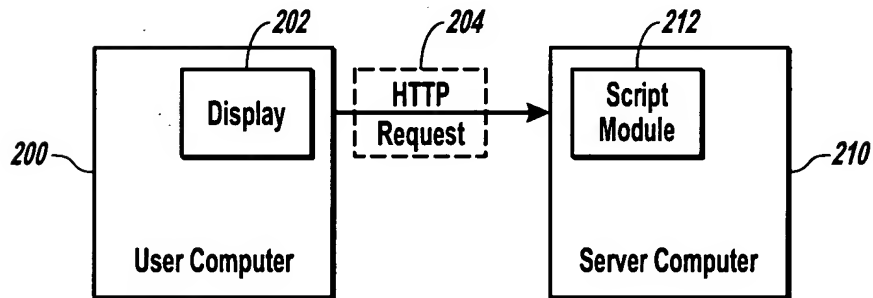Attachments: Replacement Sheet

Annotated Sheet Showing Changes

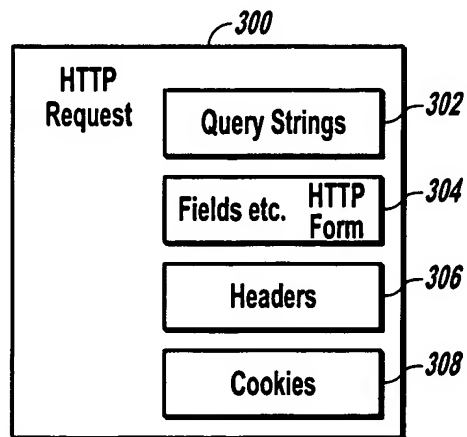Title: SYSTEMS AND METHODS FOR MITIGATING CROSS-SITE SCRIPTING
Inventor: Erik Olson, David S. Ebbo, Susan Warren, Nikhil Kothari,
Scott Guthrie, Peixin Han and Dmitry Robsman
Docket No.: 13768.373
ANNOTATED SHEET
1 / 1

**Fig. 1**
*(Prior Art)*



**Fig. 2**



**Fig. 3**